Norma de Seguridad en Desarrollos del Grupo FCC

Julio de 2025

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Abril 2009	IS	Creación del Documento	Chief Information Security Officer (CISO)
	Octubre 2019	IS	Revisión del Documento	Chief Information Security Officer (CISO)
2.0	Julio 2021	IS	Revisión del Documento Unificación del formato con el resto de la Normativa. Actualización: • Externalización del desarrollo de Software • Seguridad en las pruebas de desarrollo	Chief Information Security Officer (CISO)
2.1	Mayo 2024	IS	Revisión del documento y adaptación a la normativa ISO27001:2022	Chief Information Security Officer (CISO)
2.2	Julio 2025	IS	Revisión del documento y adaptación a la normativa ISO27001:2022	Chief Information Security Officer (CISO)

ÍNDICE

1. Introducción

El presente documento forma parte del Marco Normativo de Seguridad de la Información del Grupo FCC, que desarrolla los preceptos de obligado cumplimiento en el Grupo en materia de Seguridad de la Información.

El Marco Normativo de Seguridad es revisado y actualizado periódicamente por el departamento de Seguridad de la Información (en adelante departamento de SI), de acuerdo con lo establecido en el Documento de Gestión y Mantenimiento del Marco Normativo. Este documento contiene información sobre el historial de versiones, revisiones y aprobaciones de la presente Norma, así como su relación y dependencia con el resto de los documentos normativos.

Esta norma será revisada, por lo menos, anualmente, salvo que existan circunstancias que recomienden o exijan una revisión antes de dicha fecha.

1.1 Objeto

La presente Norma tiene por objeto asegurar que los procesos de desarrollo y mantenimiento de las aplicaciones y programas que tratan información del Grupo FCC se realicen en un entorno seguro que integre los atributos de confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad a lo largo de todo su ciclo de vida.

Se entiende como entorno seguro a las personas, procesos, tecnologías e infraestructuras relacionadas con el desarrollo e integración de los sistemas.

1.2 Alcance

La presente Norma se aplica a los proyectos de desarrollo y mantenimiento de aplicaciones, además de programas utilizados en el Grupo FCC, en adelante FCC, con independencia de donde tengan lugar y del personal que participe en los mismos.

A lo largo de la presente Norma, la expresión “proyecto/s de desarrollo de sistemas de información” hace referencia, indistintamente, al desarrollo de nuevos sistemas de información para FCC, así como al mantenimiento de los sistemas de información existentes en el Grupo.

2. Desarrollo

2.1 Principios para el Desarrollo Seguro

- Las medidas de seguridad que se apliquen a la Información de FCC tratada en proyectos de desarrollo de sistemas de información deberán ser proporcional al nivel de clasificación exigida a la misma.
- Los proyectos que impliquen desarrollo de software deberán utilizar una metodología adecuada para la implementación de las medidas de seguridad en los mismos, tanto si son realizados por personal interno como colaboradores del Grupo FCC, con la finalidad de obtener aplicaciones y programas que tengan el nivel de seguridad necesario.
- Los responsables del desarrollo de un sistema de información deberán gestionar adecuadamente los controles derivados de la implantación de la Política de Ciberseguridad y Seguridad de la información del Grupo FCC y de las necesidades definidas por el negocio.
- Los proyectos de desarrollo de sistemas de información deberán tener lugar únicamente sobre entornos de desarrollo, de pre-producción y pruebas.
- En los casos que sea necesario utilizar datos de producción durante el desarrollo o para la realización de las pruebas, las medidas de seguridad de estos entornos deberán respetar los requisitos establecidos en la Norma de Seguridad en Contraseñas, la Norma de Control de Accesos y la Norma de Criptografía, así como la normativa legal vigente.
- El desarrollo de sistemas de información y/o software por parte del Grupo FCC deberá tener en cuenta el Procedimiento de Privacidad desde el diseño y por defecto aprobado por el Grupo, así como la normativa aplicable en protección de datos.
- Los entornos de producción deberán estar convenientemente separados, por medios lógicos, de los de desarrollo y pruebas, asegurando la confidencialidad de la Información de FCC albergada en los entornos de explotación.
- Las aplicaciones deberán ser actualizadas de acuerdo con:
    - Las condiciones tecnológicas que indiquen los fabricantes.
    - Los cambios en las funcionalidades relativas a seguridad de la información.
    - Los requisitos legales que correspondan en cada momento.

- Los sistemas de información de libre disposición deberán ser adquiridos en sitios oficiales y seguros.
- Todos los cambios que se realicen en los sistemas de información deberán:
  - Estar debidamente autorizados por el responsable de la información.
  - Tener debidamente documentadas la funcionalidad interna y de las interfaces de la aplicación, la ubicación del código fuente incorporado y los registros de la operativa realizada.
- Los responsables deberán proporcionar al personal de FCC solamente aquella información que sea necesaria para la realización de su trabajo dentro del proyecto de desarrollo.
- Los ficheros temporales y de pruebas generados en estos proyectos deberán cumplir con las medidas de seguridad exigidas por el nivel de clasificación de la Información del Grupo FCC que contuvieran.
- Para el desarrollo de cualquier software se debe seguir las guías de desarrollo seguro correspondiente según el lenguaje de programación utilizado.

2.2 Seguridad de la Información en las Actividades de Desarrollo

Con carácter general, los proyectos de desarrollo de sistemas de información que se realicen en el Grupo FCC deberán:

- Emplear metodologías suficientemente probadas de análisis, diseño, implantación, generación de documentación y pruebas de desarrollo, que permitan desarrollar sistemas de información con la seguridad establecida por el Marco Normativo de Seguridad de la Información del Grupo FCC.
- Mantener actualizadas la herramientas y entornos de desarrollo integrados (IDE por sus siglas en inglés).
- Asegurar adecuadamente la seguridad de la Información del Grupo FCC, a lo largo del ciclo de vida del proyecto.
- Durante el desarrollo de sistemas de información se utilizarán las mejores prácticas de programación y se documentará el código con el objetivo de eliminar defectos y evitar que se puedan explotar vulnerabilidades.
- Formar adecuadamente a los usuarios tanto técnica, como funcionalmente en la utilización de las nuevas aplicaciones.

- Cumplir con el Marco Normativo de Seguridad de la Información en el proceso de migración de sistemas de información desde un entorno de desarrollo a uno de integración o explotación. La migración de desarrollos de sistemas de información a un entorno de producción deberá producirse de forma que este proceso no interfiera en la disponibilidad de la información.
- Asegurar que todos los desarrollos propuestos para un sistema de información son revisados a fin de comprobar que no comprometen la seguridad del mismo o del entorno operativo. Estas revisiones se realizarán de forma periódica tanto durante el desarrollo como al finalizar este.
- Realizar una adecuada gestión de cambios y control de versiones de software, en conformidad con la Norma de Control de Configuración y del Cambio.
- Las modificaciones que se realicen en las aplicaciones comerciales utilizadas por el grupo FCC deberán tener en consideración las implicaciones de índole técnica y de mantenimiento postventa, debiendo estar suficientemente documentadas para facilitar la instalación de posteriores versiones de la aplicación.
- Una vez finalizados los proyectos de desarrollo de sistemas de información, se deberá custodiar el acceso a el código fuente para protegerlo de accesos no autorizados y cualquier manipulación.

2.3 Desarrollo de Funcionalidades de Seguridad de la Información

Los proyectos de desarrollo de sistemas de información realizados en el ámbito de FCC deberán tener en cuenta la necesidad de:

- Introducir los requisitos de seguridad desde la etapa de análisis funcional de la aplicación.
- Equipar a las aplicaciones con requisitos de seguridad como los mecanismos de identificación, autenticación, control de acceso, registros de auditoría, o registros de actividad que permitan salvaguardar la seguridad de la información tratada por ellas.
- Incluir mecanismos que sean capaces de mantener el control en el tratamiento de la Información del Grupo FCC e informar de los errores producidos durante su procesamiento, preservando así la integridad y la disponibilidad de dicha información.
- Asegurar la integridad de la información tanto almacenada como en transmisión.
- Elaborar la documentación funcional y de seguridad correspondiente a las etapas de análisis y diseño de los desarrollos

- Realizar evaluaciones de seguridad con el fin de auditar la seguridad de las aplicaciones y resolver posibles vulnerabilidades.

2.4 Externalización del Desarrollo de Software

Los desarrollos externos deben realizarse bajo un contrato que regule los acuerdos de licencias, la propiedad del código y los derechos de propiedad intelectual relacionados con los contenidos subcontratados, además incluir especificaciones sobre los siguientes aspectos:

- Medidas de seguridad para las prácticas de diseño seguro, codificación y pruebas.
- Realización de pruebas de aceptación de calidad y de adecuación de las entregas, en base a los umbrales de seguridad y niveles mínimos aceptables de privacidad.
- Entrega de evidencias de la realización de pruebas para proteger los datos implicados frente a la presencia de contenido malicioso, tanto intencionado como no intencionado y contra la presencia de vulnerabilidades conocidas.
- Acuerdo de depósito en garantía, por ejemplo, si el código fuente no está disponible, derecho contractual para auditar procesos y controles de desarrollo.
- Documentación real del entorno de compilación utilizado para crear los entregables.

Así mismo, se debe establecer un marco de requisitos y controles de seguridad que se centren en la definición de los controles de seguridad funcionales y no funcionales necesarios a la hora de diseñar, desarrollar y probar el cumplimiento de las aplicaciones y servicios web. Para ello se utilizará un estándar que defina un proceso de desarrollo ágil como marco para definir las tareas específicas que debe implementar el equipo para tener un producto seguro.

Este estándar debe definir adecuadamente las vulnerabilidades de seguridad y garantizar la localización y eficacia de los controles de seguridad.

Las nuevas aplicaciones deben ser registradas en el inventario de activos del Grupo FCC, incluyendo la información acordada y la asociación entre la aplicación y:

- Los procesos de negocio que implementan.
- Sistema de información.
- Plataforma donde se ejecutan.

2.5 Seguridad en la Pruebas de Desarrollo

2.5.1 Pruebas de seguridad

Durante la fase de implementación y codificación de la aplicación, se recomienda que el área de desarrollo realice continuamente pruebas unitarias de seguridad sobre el código generado, con el objetivo de detectar y corregir posibles vulnerabilidades de seguridad lo antes posible.

Como paso previo a la producción de aplicaciones, también se debe realizar un conjunto definido de pruebas de seguridad sobre las mismas con el fin de verificar el cumplimiento de los requisitos de seguridad previamente especificados. Estas pruebas contemplarán pruebas de seguridad de caja negra (sólo a nivel de interfaces de acceso) y de caja blanca (a nivel de código fuente).

Las pruebas de aceptación del sistema deben incluir las evidencias de la realización de las prácticas de desarrollo seguro del sistema y requisitos mínimos de seguridad. Las pruebas también deben llevarse a cabo sobre los componentes recibidos y los sistemas integrados. El Grupo FCC puede utilizar herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidad, y verificar la solución de las carencias relacionadas con la seguridad.

Las pruebas deben realizarse en un entorno de prueba realista para asegurar que el sistema no va a introducir vulnerabilidades al entorno de la organización y que las pruebas son fiables.

2.5.2 Datos de carácter personal para las pruebas

Las pruebas relativas a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

3. Responsabilidades

El departamento de SI deberá:

- Definir las funcionalidades de seguridad que deben de ser implantadas en las aplicaciones y programas.
- Verificar que las funcionalidades de las aplicaciones y los entornos de desarrollo cumplen con los requisitos establecidos en las normas de seguridad emitidas por el Grupo.
- Monitorizar las amenazas del mundo real para asesorar y actualizar la información sobre vulnerabilidades de software en aras de guiar a la organización a través de principios de codificación segura y procesos de mejora continua.

La División de Sistemas y Tecnología de la Información deberá:

- Implantar las medidas técnicas y organizativas necesarias para proteger la seguridad de la información tratada en los proyectos de desarrollo.
- Integrar los requisitos de seguridad dentro de las funcionalidades de las aplicaciones y programas.
- Validar las pruebas técnicas realizadas sobre las aplicaciones y programas, verificando que se cumplen las funcionalidades de seguridad exigidas.
- Efectuar una gestión de inventario completa y actualizada periódicamente de las aplicaciones, entornos y versiones del software.

Los Responsables de la Información deberán:

- Proponer medidas para mejorar las funcionalidades de seguridad de los desarrollos de los sistemas de información de FCC.
- Validar las pruebas de las aplicaciones y programas con la finalidad de asegurar que las funciones de seguridad son las definidas en el análisis de requisitos de seguridad.4. Referencia a la normativa interna del grupo FCC.

4. Referencia normativa

El presente documento ha sido revisado por el departamento de SI y su redacción toma como referencia el estándar internacional ISO27001:2022 y ENS.

4.1 Controles de la normativa ISO27001:2022 y ENS

ID Control ISO	Control ISO/IEC 27001:2022	Correspondencia ENS
8.27	Arquitectura del sistema seguro y principios de ingeniería	[op.pl.2] Arquitectura de Seguridad; [mp.sw.1] Desarrollo de aplicaciones
8.28	Codificación segura	[mp.sw.1] Desarrollo de aplicaciones
8.29	Pruebas de seguridad en desarrollo y aceptación	[mp.sw.2] Aceptación y puesta en servicio
8.30	Desarrollo subcontratado	[op.ext.1] Contratación y acuerdos de nivel de servicio; [op.ext.3] Protección de la cadena de suministro; [mp.sw.1] Desarrollo de aplicaciones; [mp.sw.2] Aceptación y puesta en servicio
8.31	Separación de los entornos de	[mp.sw.2] Aceptación y puesta en servicio

	desarrollo, prueba y producción	
8.32	Gestión de cambios	[op.exp.5] Gestión de Cambios
8.33	Información de prueba	[mp.sw.1] Desarrollo de aplicaciones; [mp.sw.2] Aceptación y puesta en servicio